From the Internet of Things to the Internet of People

Javier Miranda, Gloin, Niko Mäkitalo, Tampere University of Technology, Jose Garcia-Alonso, University of Extremadura, Javier Berrocal, University of Extremadura, Tommi Mikkonen, Tampere University of Technology, Carlos Canal, University of Malaga, and Juan M. Murillo, University of Extremadura

Abstract

There is growing interest in developing applications on the Internet of Things. These applications' main objective is to integrate technology into people's everyday life in order to be of service to them en masse. The form in which this integration is implemented, however, still leaves much room for improvement. Usually, the user needs to set parameters within the application. When the person's context changes, they have to manually re-configure the parameters. What was meant to be a commodity, in an unforeseen situation then becomes extra noise. This paper describes a reference architecture that improves how people are integrated with the Internet of Things, with smartphones doing the connecting. The resulting integration opens the way to new IoT scenarios supporting evolution towards the Internet of People.

Keywords: Internet of Things, Internet of People, mobile devices, sociological profiles, pervasive computing, sensors, adaptation to user state, affective computing

1 Introduction

Today's availability of the Internet almost everywhere has favoured the emergence of all kinds of devices equipped with a connecting interface. Linking those and other everyday physical objects to the Net is getting ever easier, thus enhancing the popularity of the Internet of Things (IoT). One of the main goals behind such smart integration of devices is to simplify people's lives by having technology work for them seamlessly [1]. For instance, you can remotely switch on your house's air-conditioning system using your smartphone to get a comfortable temperature when arriving home. Or you might schedule this task in accordance with your daily routine.

However, how IoT technologies are currently integrated with humans still leaves much room for improvement [2]. The technology has yet to develop suitable mechanisms to properly adapt to people's context or mood. Instead, far from making the technology working for people, people are forced to either change their context to fit technological requirements, or to be slavishly aware of the system so as to send it commands or modify their schedule if their routine changes.

In a more desirable IoT scenario, technology would take people's context into account, learn from it, and take proactive steps according to their situation and expectations, avoiding user intervention as much as possible. Thus, if someone plans to arrive home late, they would like the air-conditioning kept switched off until they are actually on their way back home.

Enabling such scenarios requires moving from the Internet of Things to the *Internet of People* (IoP). This article proposes an infrastructure supporting this evolution, and making it possible to construct software for it. In our proposal, smartphones play a central role, reflecting their current use as the main interface allowing people to be connected to the Internet. Thus, we advocate endowing smartphones with a set of capabilities that improve the connection between people and the IoT. First, the smartphone needs to be capable of learning about its owner and their context by constructing their digital profile (understood as the whole of the context information managed by the device). Second, it needs to transparently negotiate and propose interactions with other devices on the Internet, reacting to stimuli and handling relationships. Finally, it needs to be able to manage digital profiles and act accordingly, providing its owner's context as a service for others, and scanning for services that might be of interest to its owner or to update his or her digital profile.

The infrastructure to support the IoP is managed through a combination of the Social Devices [3] and People as a Service (PeaaS) [4] platforms. Social Devices enhances the proactive capabilities of smartphones to orchestrate their interactions with other devices connected to the IoT. PeaaS provides smartphones with serving capabilities that allow people to offer services from their devices, including providing their context and sociological profile. The combination of the two contributes to constructing an IoP by allowing people's context information to be included in the coordination and interaction management of IoT devices. The main benefit is the integration of people as first-class citizens in the IoT universe. This opens the way to the development of new kinds of human-friendly services and applications in the field.

2 People are not Things

The IoT is increasingly pervading our daily lives. Currently 12.6 billion connected devices are estimated [5], including people, processes, data, and things. This last "connected things" group includes not only mobile devices such as smartphones or tablets, but also desktop and laptop PCs, printers, smart TVs, cars, refrigerators, smart light bulbs, etc. IoT numbers are increasing at a dizzying pace. Experts [6] forecast 25 billion connected devices in 2020. Even devices that do not come equipped with a connecting interface can easily be integrated into an IoT system using such hardware platforms as Arduino, .NET Gadgeteer, or even Lego Mindstorms for kids.

The complexity and heterogeneity of such a large variety of smart devices that can be connected to the Internet requires specific tools to manage them. Current approaches, at least within the industry, have merely been based on offering remote interfaces and endpoints to configure and manage devices, leading to the "Basket of Remotes" problem [7].

The need to combine interactions between several devices led to the development of Machine-to-Machine (M2M) communications. There have been attempts at standardization, such as DPWS [8] and CoAP [9]. While user-friendlier approaches, such as Apple's HomeKit, help integrating home automation via smartphones, they are still in the development stage.

For practical applications, individual gadgets alone are insufficient. Instead, many real-life applications connect devices into cloud computing and storage facilities, enabling the creation of arbitrarily complex systems in which nodes, ranging from sensors to data centres, perform computations. This architecture is a natural starting point for creating mashups that combine data from various sources into new, compelling ways to consume those data. It has, for instance, rapidly become a practical way to keep track of personal sports activities and interests.

However, although the problem of accessing, programming, and combining IoT objects can be settled with a cloud-based architecture, making them accessible to a broad spectrum of users, the way that IoT devices are related to people, still requires more attention. Current tools and technologies supporting the interaction between humans and IoT force the user to adapt to technology, instead of making technology adapt and assist the user. As the user's circumstances change, a conductor is required to manage the orchestra of IoT-linked devices, and reduce the complexity of user interaction with them. In our opinion, such a role can be successfully performed by smartphones. They are the natural interfaces to their owners, connecting them to the outside world. Due to their intrinsically personal nature, smartphones are almost always on their owner's person, and their capabilities, geolocating in particular, can be used to learn about the person's context, i.e., to detect how the person behaves when they are at certain locations, surrounded by certain other people, and so on. Combined with smartphones' growing computing capabilities, it makes them ideal for learning about people and orchestrating their surrounding IoT. Still, every interaction involving people should be casual and hassle-free, giving the user full control of private data so that the interactions are perceived as taking place between the people, and not between the things, connected to the Internet.

3 Background (sidebar)

3.1 Social Devices

Social Devices was first introduced in 2011 as a joint work by Nokia Research Center, Aalto University, and Tampere University of Technology [3]. The motivation behind the model was that smartphones have not only a lot of information about their owners, but also modalities that enable them to resemble humans. They can translate text into speech, for example. At present, the Social Devices concept is supported by a middleware platform named Orchestrator.js (`http://www.orchestratorjs.org`). This allows proactive triggering of interactions between devices of co-located people. Additionally, it offers a complete set of Web-based tools to define the interactions and their triggering contexts. Currently, the middleware allows custom IoT smart objects to be constructed using Arduino, Raspberry Pi, or .NET Gadgeteer. Work is on-going to extend the support to new platforms since the goal of Social Devices is to allow heterogeneous multi-user and multi-device applications to be created for any type of device.

Various IoT-related scenarios have been implemented and introduced using Social Devices. One example is The Social Coffee Machine. This, based on user context, asks if the user wants to have coffee, and then, when the coffee is ready, invites other people to join the coffee break.

3.2 People as a Service

People as a Service (PeaaS) [4] is a mobile-centric computing model that allows a user's sociological profile to be generated, kept, and securely provided as a service to third parties directly from a smartphone.

PeaaS emphasizes smartphones' capabilities, and relies on them for inferring and sharing sociological profiles. These are kept on the device, making it easier for the owner to keep their virtual identity under their own control while still allowing external systems to consult those identities.

Serving individuals' virtual sociological profiles through smartphones goes one step beyond other mobile-centric models that only serve data such as GPS coordinates and temperature. PeaaS allows a variety of information to be collected, such as the moods, trends, social statuses, and health habits of a group of people, in order to define their digital projection. However, filtering and analysing that information to infer user's characteristics or to extract useful data is not a trivial task. Different techniques, including activity recognition approaches [10] and affective computing [11], are considered in PeaaS for building the richest sociological profile as possible.

Current mechanisms used to specify the orchestration of smart-things could take advantage of the final user's sociological profile to suggest (or even automatically provide) a customized IoT workflow in accordance with the user's likes and preferences. Similarly, in events in a smart-city context, the set of sociological profiles extracted from a crowd could be applied to automatically redirect people so as to avoid unnecessary agglomerations.

The PeaaS model is currently implemented as component of a mobile notification platform named nimBees (`http://www.nimbees.com/`), which provides smart push notifications with advanced segmentation capabilities based on user's sociological profile.

4 Internet of People Manifesto

As noted above, current IoT technology is in need of people-centric enhancements. Our proposal is intended to be a step in this direction. It conforms to a set of features that we believe to be essential foundations for any approach to the IoP. In this section, we shall put forward four guidelines for an IoP Manifesto in terms of the desirable service composition goals for any pervasive computing context (context awareness, contingencies management, heterogeneity and empowering of the users), as set out in [12].

4.1 Be Social

Interactions in which things, devices, and people participate must be social. In particular, the IoP should allow for heterogeneity by supporting the different types of devices that people use, and let them interact with each other and with people more socially than does the IoT. Devices will have to be context-aware and capable of automatically adapting their own and other devices' social behaviour. Users need to be empowered to adjust their preferences and policies about when and with whom their devices are socializing, and with which modalities.

4.2 Be Personalized

Interactions between devices must be personalized to the sociological profiles and contexts of their users, allowing for contingencies, and providing a transparent mechanism for this customization. The sociological profiles of all participating people must be taken into account. Again, users must be empowered to adjust their preferences in order to control how other IoP stakeholders use their profile.

4.3 Be Proactive

The triggering of interactions must be proactive, not manually commanded by the user. Most IoT scenarios today only consider remote interfaces for managing connected things. But ever more things online mean more distractions and work in managing them. The IoP should allow for device heterogeneity to allow them all to interact more proactively. Users must be empowered to adjust their preferences to control how proactive their surrounding things are. It should be noted than letting devices to act proactively could entail security risks that must be analysed and delimited, keeping users informed of any established proactivity policy.

4.4 Be Predictable

Interactions must be predictable, i.e., they should be triggered according to a predictable context that the user had previously identified, and for which a specific behaviour had been defined. Users must be empowered to identify and tag that context, specify the expected behaviour of the things involved, and set the privacy policies for sharing their information by being advised of what information they are sharing and with whom. As complete predictability of interactions is very hard to achieve, the user needs to always understand how the interaction can be stopped immediately, like whacking your phone as proposed in [13], and also how this misbehaviour can be prevented in future.

5 Internet of People Blueprint

We have designed a reference architecture supporting our vision of the IoP, based on the PeaaS and Social Devices platforms. The result is a more human-like and less user-dependent IoT ecosystem. The architecture is a natural consequence of the objectives set out in the IoP Manifesto. As illustration, we shall consider a particular case study scenario.

5.1 Scenario: Smart Transportation

David lives in a residential suburb of Paris. Like every day, he is driving his daughter to school before going on to work. His smartphone has learnt where he lives, where he works, and the route he usually takes and at what time. It has reported this information to the city's transportation control systems. David is happy to anonymously contribute such information since it is used for simulations and previsions of potential traffic problems, and to plan improvements in the city.

David has no need to interact with his smartphone because, when he left home this morning, it already knew where he was going. This was confirmed when it detected that the route and speed were as usual. Unfortunately, a traffic accident has just occurred, and David is stuck in a jam. His smartphone has detected an abnormally low speed at a certain point of his route. It asks the smartphones of people around whether they are stuck too. On confirmation, it alerts the transportation control systems of a possible incident. Since every smartphone is reporting the same issue, the control system raises a traffic alert, and notifies the smartphones of people usually take the same route, suggesting an alternative. David's smartphone is now receiving information about the new route to follow, and the estimated time of arrival. It then passes the new route to the car navigator that immediately informs David about the best way out of the jam. The smartphone knows that David is now late and reports to his office, indicating the expected time of arrival.

Most of the people behind David manage to avoid the jam, and David arrives only ten minutes late. He is not too unhappy because he recalls the days when smartphones were only used to talk, read emails, and surf the Web during traffic jams. He is also pleased to have contributed to reducing the impact of the traffic jam for his neighbours.

5.2 Internet of People Middleware

Figure 1 shows a high-level architectural description of the IoP middleware, conceived as a service-oriented system comprising various components: a Device Registry, an Application Manager, an Application Repository, and an Action Repository.

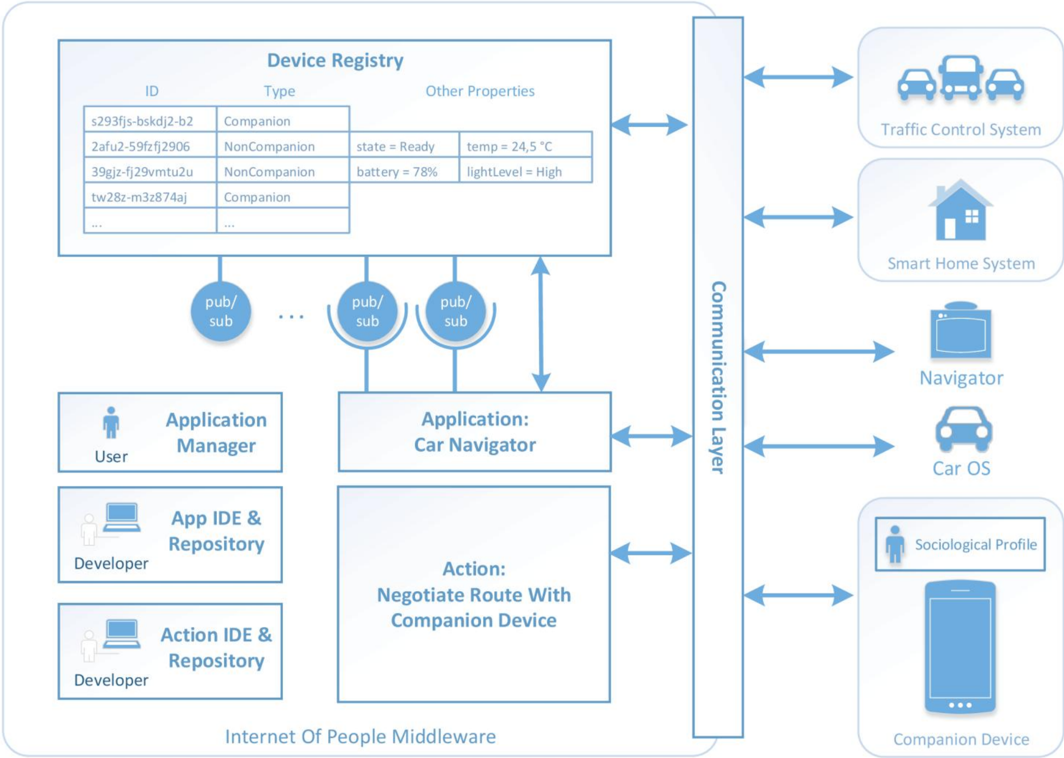

Figure 1: Internet of People Middleware

The central component is the Device Registry. This maintains the information about the different devices managed by the system. These devices are classified into Companion and NonCompanion.

Companion devices are those that maintain contextual and sociological information about their owners, and serve that information through the implementation of the Sociological Profile component inside them. In the illustrative scenario, David's smartphone is registered as a Companion device in the IoP context to allow interactions with other things in that context, such as surrounding people's smartphones or his car navigator. Identifying smartphones as Companion devices in the IoP registry allows them to be considered as representations of people in the IoP context, and, if they are socially capable devices, as conforming to the Manifesto's "be social" principle.

NonCompanion devices are those without a Sociological Profile component. They are "things" which can register their capabilities and any additional information about their state, including any sensing properties and values. The registry incorporates a publish-subscribe API mechanism to allow monitoring the state and property changes of the registered devices. In our scenario, things like car navigators and the traffic control are registered as NonCompanion devices They publish their properties' values in the registry to allow the IoP system to take the appropriate measures according to monitoring rules, such as alerting the smartphones of people close to a traffic jam. This behaviour conforms to the Manifesto's "be proactive" principle.

The Action Repository component manages the middleware's set of actions. Each action defines how the devices should interact with each other and with people. The Application Repository component stores the different applications defined in the IoT context and managed by the IoP middleware. An application consists of a set of instructions defining under what conditions to trigger a set of actions and which devices will be involved. An application's triggering conditions can be defined by monitoring the changes in the state of one or more devices using the registry's publish-subscribe API protocol. In the smart transportation scenario, that mechanism allows an application to be written to monitor the state of the traffic reported by the traffic control system and to trigger the appropriate actions to redirect people in the traffic jam.

The Application Manager component allows people to enable or disable the different applications according to whether they would like to be present and contribute with their sociological profiles.

The application and action specifications may include requests to the different Sociological Profile components of the Companion devices involved, so that the specified behaviour can be adapted to the user's context, personality, or mood.

5.3 Sociological Profile

The Sociological Profile component is a fundamental part of every Companion device. This component maintains the information that has been gathered and inferred about people and their contexts. This information covers people's behaviour, preferences, and also raw contextual data such as current or historical locations, sensing information (e.g. accelerometer status), and processed contextual information such as a proximity graph of surrounding people/devices/things. In the smart transportation scenario, David and other users' Companion devices detected a delay on their route on the basis of their location, movement information, and expected arrival time according to the behavioural pattern data of their sociological profiles.

This component serves information in response to requests via a query-based service. When it receives a request for information about some property stored in the Sociological Profile, it is answered by the Companion device, providing that information as a service response. Companion devices can also notify the registry about significant changes in their Sociological Profile, so that subscribed applications will be notified when an on-change event occurs, allowing them to re-run the queries to get the freshly updated information. In the smart transportation scenario, David's smartphone uses this mechanism to ask nearby people's smartphones for verification of the traffic state.

The component also allows users to define and adjust the sharing schema for the profile. Users should define what information will be available for which applications, devices, or users, and in which context the information should be provided. In the smart transportation scenario, David's smartphone shares his daily route with his workplace, but makes it inaccessible for other systems. Such privacy rules align this approach with the Manifesto's "be predictable" principle.

Finally, the Sociological Profile provides an interface for device owners to personalize the way in which the device behaves under specific circumstances. In the smart transportation scenario, when the traffic control system notifies people's smartphones about the traffic jam on their route, their profiles can mould the resulting alarm action by translating the message into their native language, and shaping the voice to the proper accent, timbre, or mood according to their profile information and context. This conforms with the Manifesto's "be personalized" principle.

Most of the profile's customizable policies and preferences will be supported by a user-friendly wizard. The component will progressively learn the customization during the device's use from the interactions and contexts in which it is involved, and from the owner's decisions about how the device should behave in those interactions. In the smart transportation scenario, David's device recognized a previously learnt pattern about his daily driving routine, which made it possible to detect deviations, and react accordingly. This behaviour also conforms to the Manifesto's "be predictable" principle.

5.4 Building Proactive Interactions

Many IoT and pervasive service systems have their own communication protocols and ways of interconnecting objects. But they typically overlook how the "things" interact with people. To construct more human-like, predictable, proactive, and social interactions between people and "things", the IoP middleware offers a Web-based IDE and tools. These tools allow applications to be constructed to monitor user context, and then, based on the user's context, proactively trigger interactions between the people and "things" involved. Two examples in the smart transportation scenario might be that when the Companion device receives an alert, it can read it aloud for the owner while he is driving, and that the smartphone and the navigator can inform the user while rerouting the way to work so that David can be aware of what is going on. These tools, and the development effort for building new devices and applications has been described in [14] and `http://orchestratorjs.org`.

6 Discussion and Concluding Remarks

The success and growth of IoT is unquestionable. However, people's interaction with this kind of systems is still far from friendly. We have here presented a reference architecture to smooth out how people relate with

IoT systems. By basing people's interactions with the system through their smartphones, our proposal reduces the complexity inherent in the IoT, contributing to evolution towards a true IoP.

The term Internet of People has been used before, but usually to refer to traditional Web systems designed only for humans to use. Here, we have used it in the sense of bringing the Internet of Things closer to people, for them to easily integrate into it and take full advantage of its benefits. Technologies such as Siri for iOS or Sherpa for Android have endowed smartphones with a kind of persona. The next step could be to adjust this persona to fit the user's personality and mood.

This potential use of smartphones as personal information gatherers and managers, and conductors of orchestras of other devices, has also motivated other research initiatives. As well as the aforementioned PeaaS and Social Devices, in [15] smartphones are seen as service providers, with an implementation based on Web Service standards interfacing the user with other smartphone services. This could provide a mechanism for serving user's contextual information, but the management of IoT devices, as provided by the IoP approach, is out of its scope. Paraimpu (`http://www.paraimpu.com`) provides a social tool for people to connect, compose, and share things, services, and devices to create personalized IoT applications. Node-RED (`http://www.nodered.org`) provides a Web-based visual interface for connecting and building compositions of hardware devices, APIs, and online technical and social services. Both works deal great with IoT management but they lack on the predictability and sociological profile features provided in the IoP approach. Apple HomeKit promises integration with a large set of compatible devices, and managing them remotely, but it is also a platform-specific solution.

We have presented here a manifesto to encourage other IoT system developers and researchers to pay attention to the relation between people and IoT systems. As noted above, the architecture proposed here is based on combining the existing Social Devices and PeaaS proposals. Currently, Orchestrator.js and nimBees are consolidated implementations that complement each other in Internet of People middleware. Later on, other systems, like recommendation systems for instance, can be applied to our approach.

The maturity of our previous work allow supporting interactions between people and household devices based on pattern recognition applied to smartphone usage. For example, we can now turn on a coffee machine when a user starts her journey to work. The implementation of scenarios, such as the smart transportation one, enables addressing possible scalability issues.

The major privacy and socially related questions that proposals such as ours raise will set a new horizon for research in the coming years. Our own future work plans focus on taking advantage of the ever-increasing capabilities of smartphones so as to improve how they make inferences about their owners, and to use that information to enhance their owners' roles in IoT systems.

Acknowledgments

This research has been partially funded by the Spanish government (projects TIN2012-34945, and TIN2012-35669), the Academy of Finland (264422) and by Nokia Foundation. It has also been funded by the Government of Extremadura and the European Regional Development Fund (FEDER).